Technical Cybersecurity

Scanning

Why?

WE NEED TO KNOW WHAT WE CAN ATTACK

- Network topology: Useful for pivots, common services
  - Not all systems are created equal
- Learn what we have access to
  - What ports are open? what service are being used?
  - Mail is more valuable than DNS!
- Find vulnerabilities

Attacking? Find targets (and exploit).
Defending? Find targets (and patch).

Using NMAP

Time to get our hands dirty!

- We’re going to start scanning systems. We already have two in your lab (three, if you want to scan your workstation :-))
- This isn’t very many systems!
  - This is true.
  - …the techniques you use scale to a point
  - …and when they stop, you can use something like **masscan**
  - Mass scanning is usually only for initial network mapping, not detailed analysis

Onto NMAP!